UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,765	07/07/2003	Paul C. Kocher	2007003 / CRYP2CIP1US	8024

73091 7590 10/22/2008

Marc P. Schuyler
P.O. Box 2535
Saratoga, CA 95070

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/614,765	**Applicant(s)** KOCHER ET AL.	
	Examiner JEFFREY D. POPHAM	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _23 July 2008_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _2-25_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _2-25_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _07 July 2003_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _20080604_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Remarks

Claims 2-25 are pending.

Response to Arguments

1. Applicant's arguments filed 7/23/2008 have been fully considered but they are not persuasive.

Applicant argues that none of the cited art discloses security check features performed by program logic in the manner defined by claim 22. Of note is the wording of claim 22, providing that the program logic is adapted to perform this at least one security check of a playback device seeking to play the audiovisual content, the at least one security check adapted to verify at least one of playback device identity, including at least one of a player serial number, specific subscriber information, player model, or player software version, or a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device. One can see that the decryption instructions that are stored on the medium of the combination (such instructions in Kyle) comprise cryptographic processing, and that such cryptographic processing is adapted to fail if the device cannot decrypt the data (such failure more easily seen in Asano where decryption fails if the device does not have the proper key(s)). There are other security checks within the references as well, such as Kyle, column 5, lines 21-23, stating "The decryption code would be assembled with the encrypted data only upon a request from a legitimate user", showing authentication of a user before allowing decryption to occur. Further security checks can be found in the other references regarding authentication of the device (e.g. device revocation lists), user, and data.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 2-25 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amendment to claim 1 has added program logic for an interpreter, “the program logic installing on the playback device and cryptographically protecting on the playback device the revocations list”. First, the application as originally filed does not appear to discuss any program logic that installs on the playback device. While there may be an upgrade to software, firmware, or the like included with the content, such upgrade being performed if the proper conditions exist (such as authentication of the device and content), there does not appear to be any basis for “program logic installing on the playback device" as recited in claim 1. Perhaps this is more an issue of awkward wording, though, meaning that the program logic on the medium copies the revocations list onto the device, however, the Examiner cannot find basis for that in the application as originally filed either. Furthermore, the Examiner cannot find basis for program logic “cryptographically protecting on the playback device the revocations list”. While the application as originally filed does discuss code that can verify whether the medium is revoked based on a revocations list, the program logic that is stored on a medium (as in claim 1) never cryptographically protects a revocation list on the playback device. Protecting the list would comprise the program logic itself protecting the list in some manner, such as by encrypting the list, forming a digital signature on the list, or the like, which does not appear to be described in the application as originally filed. Verifying/checking information in a list (even if said list is signed or encrypted) does not comprise protecting the list.

Claim Objections

3. Claims 12, 16, 21, and 23 are objected to because of the following informalities:

- Claim 12 recites “decrypt said selected version(s)”, however, the immediately preceding step refers to "select a version of each said region", providing only a singular version. For purposes of prior art rejection, "version(s)" has been construed as "version".
- Claim 16 has been amended to refer to “the media drive” and “said media”, which do not have antecedent basis. To be clear, reference to "revoked media" is fine, but "verifying whether valid digital signatures contained on said media" is not, since this is in reference to the

medium discussed in step (a). For purposes of prior art rejection, except as just described, "the media drive" has been construed as “a media drive” and “said media” has been construed as “said medium).

- Claim 21 is difficult to understand, and has been construed as “The medium of claim 3 where program logic is adapted to embed results of the plurality of security checks into audiovisual content rendered by the playback device on which security checking is performed”.
- Claim 23 refers to “the media verification logic”, which has been removed via amendment from claim 12 from which claim 23 depends and "interrogates playback environment", such playback environment never having been introduced in claim 12 or 23. For purposes of prior art rejection, “the media verification logic” has been construed as “logic” and “interrogates playback environment” has been construed as “interrogates a playback environment”.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-13, 15, 16, and 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano (U.S. Patent 6,999,587) in view of Benaloh (U.S. Patent 7,065,216), Nonaka (U.S. Patent Application Publication 2002/0035492), and Kyle (U.S. Patent 6,141,681).

Regarding Claim 2,

> Asano discloses a digital optical medium containing compressed digital audiovisual content with protections against unauthorized copying, comprising:
>
> A digital signature authenticating at least an identifier of the optical medium (Column 7, line 33 to Column 8, line 3);
>
> A revocations list indicating that at least one other medium is revoked (Column 8, lines 10-30);
>
> Digital audiovisual content that is encrypted using broadcast encryption, whereby: each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the audiovisual content, and each of a plurality of revoked playback devices do not have keys sufficient for decrypting the audiovisual content (Column 6, lines 29-32; Column 8, lines 45-59; Column 9; lines 35-58; and Column 14, lines 1-63); and
>
> Logic defining an interface usable to control playback of the audiovisual content (Column 6, lines 29-32; and Column 14, lines 1-63);

But does not explicitly disclose that the list contains identifiers of revoked media, program logic for an interpreter of a Turing complete language, the program logic adapted for execution on a playback device in order to play the audiovisual content, the program logic installing on the playback device and cryptographically protecting on the playback device the revocations list, a plurality of versions of a plurality of portions of the digital audiovisual content where the versions for each portion may be distinguished from each other in pirated recordings of the audiovisual content; the versions are encrypted with different keys, such that each of the authorized playback devices is capable of deciphering at least one, but not all, of the versions for each of the portions; and the combination of the portions decipherable by a given player may be used to identify the player.

Benaloh, however, discloses that the digital audiovisual content is compressed and encrypted, whereby each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the audiovisual content, and each of a plurality of unauthorized playback devices do not have keys sufficient for decrypting the audiovisual content (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12); and

A plurality of versions of a plurality of portions of the compressed digital audiovisual content, where: the versions for each portion may be distinguished from each other in pirated recordings of the audiovisual content; the versions are encrypted with different keys, such that each of the authorized playback devices is capable of deciphering at least one, but not all, of the versions for each of the portions; and the combination of the portions decipherable by a given player may be used to identify the player (Column 9, line 61 to Column 11, line 12); and

Logic defining an interface usable to interact with a user and to control playback of the audiovisual content (Figure 1; and Column 3, line 24 to Column 4, line 40). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the digital content protection scheme of Benaloh into the information recording/reproducing system of Asano in order to allow the system to detect pirated copies of content and trace it back to the specific player used to pirate the content while providing all content players with identical data on the storage medium.

Nonaka, however, discloses that the list comprises identifiers of revoked media (Paragraphs 232-234) and program logic cryptographically protecting on the playback device the revocations list (Paragraphs 223-228). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the revocation methods of Nonaka into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to revoke additional entities, such as devices and media, thereby providing better assurance that media and devices are proper before allowing content usage.

Kyle, however, discloses program logic for an interpreter of a Turing complete language, the program logic adapted for execution on a playback device in order to play the audiovisual content, the program logic installing on the playback device (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; Column 7, line 59 to Column 8, line 5; and Column 9, lines 19-29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh and Nonaka in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Regarding Claim 3,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 22, in addition, Asano discloses performing a plurality of the security checks and permitting playback of the audiovisual content provided that the plurality of security checks are successful (Column 6, lines 29-32; Column 8, lines 45-59; Column 9; lines 35-58; and Column 14, lines 1-63); and Kyle discloses that the program logic is configured to perform security checks and permit playback provided that the security checks are successful (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 24; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 4,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 3, in addition, Kyle discloses that the program logic is configured to invoke at least one cryptographic operation supported by at least one of the authorized playback devices (Column 4, line 57 to Column 5, line 14).

Regarding Claim 5,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 3, in addition, Kyle discloses that the program logic is configured to perform at least one operation necessary for decryption of the audiovisual content by at least one authorized playback device (Column 4, line 57 to Column 5, line 14).

Regarding Claim 6,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 2, in addition, Kyle discloses that a subset of the authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and further comprising program logic which, when executed by a device of each vulnerable model, is configured to: mitigate the vulnerability affecting the vulnerable playback device; and perform at least one operation necessary for the vulnerable playback device to decrypt the audiovisual content (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 7,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 6, in addition, Kyle discloses that the program logic includes executable code for a Turing-complete virtual machine (Column 3, line 66 to Column 4, line 6; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 8,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 6, in addition, discloses that the operation necessary to decrypt includes updating a cryptographic key contained in the playback device (Column 12, lines 35-67).

Regarding Claim 9,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 6, in addition, Kyle discloses that the program logic for mitigating includes native executable code configured to detect whether the security of a vulnerable device has been compromised (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 10,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 6, in addition, Kyle discloses that the program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 11,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 6, in addition, Benaloh discloses that the player comprises firmware (Column 7, lines 48-53; and Column 11, lines 13-42); and Kyle discloses that the program logic for mitigating includes an upgrade to the player for correcting at least one vulnerability (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 19).

Regarding Claim 12,

Asano discloses a device for securely playing digital audiovisual content, the audiovisual content including a plurality of regions each having multiple versions thereof, comprising:

A media drive including a laser for use in reading data from rotating optical media (Column 8, lines 45-58);

A nonvolatile memory containing: a set of cryptographic player keys for use with a broadcast encryption system, and identifiers of revoked manufacturers (Column 9; lines 35-58; and Column 11, lines 18-30);

A bulk decryption module for decrypting encrypted audiovisual content from the media (Column 14, lines 1-63); and

Logic configured to verify whether valid digital signatures contained on the media authenticate the media, and whether the media are identified as revoked in the nonvolatile memory (Column 9, lines 45-67);

But does not disclose that the list contains identifiers of revoked media, a Turing-complete interpreter for executing program logic configured to install from a media drive, select a version of each region, and decrypt the selected version, whereby a combination of the versions selected in the course of playing the media uniquely identifies the device; and at least one codec for decompressing the audiovisual content.

Benaloh, however, discloses program logic configured to select a version of each region, and decrypt the selected version, whereby a combination of the versions selected in the course of playing the media uniquely identifies the device (Column 9, line 61 to Column 11, line 12); and at least one codec for decompressing the audiovisual content (Column 3, line 65 to Column 4, line 6). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to incorporate the digital content protection scheme of Benaloh into the information recording/reproducing system of Asano in order to allow the system to detect pirated copies of content and trace it back to the specific player used to pirate the content while providing all content players with identical data on the storage medium.

Nonaka, however, discloses that the list comprises identifiers of revoked media (Paragraphs 232-234) and program logic cryptographically protecting in nonvolatile memory identifiers of revoked media (Paragraphs 223-228). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to incorporate the revocation methods of Nonaka into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to revoke additional entities, such as devices and media, thereby providing better assurance that media and devices are proper before allowing content usage.

Kyle, however, discloses program logic configured to install from a media drive (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; Column 7, line 59 to Column 8, line 5; and Column 9, lines 19-29). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to incorporate the self protecting data package system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh and Nonaka in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Regarding Claim 13,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the device of claim 12, in addition, Kyle discloses an interpreter for a Turing-complete language, where the interpreter is configured to obtain program logic from the drive and execute the program logic (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 15,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the device of claim 12, in addition, Benaloh discloses that the combination of versions selected during the course of playback of any one medium does not uniquely identify the playback device; and the combination of versions selected during the course of playback of a plurality of the media does uniquely identify the playback device (Column 14, lines 41-50).

Regarding Claim 16,

Asano discloses a method for playing encrypted digital audiovisual content from a digital medium, comprising:

Verifying a digital signature authenticating the medium (Column 9, lines 45-67);

Retrieving at least one player key from a nonvolatile memory (Column 9; lines 35-58; and Column 11, lines 18-30);

Using the at least one player key with a broadcast encryption system (Column 12, lines 35-67);

Using the result of the broadcast encryption system to decrypt at least a portion of the audiovisual content (Column 12, lines 35-67; and Column 14, lines 1-63);

Program logic configured to verify whether valid digital signatures contained on the medium authenticate the medium, and whether the medium is identified as revoked in the nonvolatile memory (Column 9, lines 45-67);

But does not explicitly disclose selecting a variant from a plurality of variants for each of a plurality of portions of the audiovisual content, where: the player is capable of decrypting the selected variants, and the player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each portion; decrypting each selected variant; reading program logic for a Turing-complete interpreted language from the medium; and using an interpreter to execute the program logic, where the interpreter performs operations specified in the program logic to respond to selections from a user.

Benaloh, however, discloses selecting a variant from a plurality of variants for each of a plurality of portions of the audiovisual content, where: the player is capable of decrypting the selected variants, and the player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each portion; and decrypting each selected variant (Column 9, line 61 to Column 11, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the digital content protection scheme of Benaloh into the information recording/reproducing system of Asano in order to allow the system to detect pirated copies of content and trace it back to the specific player used to pirate the content while providing all content players with identical data on the storage medium.

Nonaka, however, discloses program logic cryptographically protecting identifiers of revoked media (Paragraphs 223-234). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the revocation methods of Nonaka into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to revoke additional entities, such as devices and media, thereby providing better assurance that media and devices are proper before allowing content usage.

Kyle, however, discloses reading program logic for a Turing-complete interpreted language from the medium; and using an interpreter to execute the program logic, where the interpreter performs operations specified in the program logic installing from a media drive (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh and Nonaka in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Regarding Claim 19,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the method of claim 16, in addition, Asano discloses accessing a media revocations list to determine whether the medium has been revoked (Column 8, lines 10-30; and Column 9, lines 35-67); and

Nonaka discloses that the list comprises identifiers of revoked media (Paragraphs 232-234).

Regarding Claim 20,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the device of claim 12, in addition, Benaloh discloses that the set of cryptographic player keys is unique to the player and the program logic is configured to select a unique set of versions representing the content using the unique set of cryptographic player keys (Column 9, line 61 to Column 11, line 12).

Regarding Claim 21,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 3, in addition, Benaloh discloses that the program logic is adapted to embed results of the plurality of security checks into audiovisual content rendered by the playback device on which security checking is performed (Column 9, line 61 to Column 11, line 12).

Regarding Claim 22,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the medium of claim 2, in addition, Asano discloses at least one security check of a playback device seeking to play the audiovisual content, the at least one security check adapted to verify at least one of playback device identity, including at least one of a player serial number, specific subscriber information, player model, or player software version, or a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device (Column 6, lines 29-32; Column 8, lines 45-59; Column 9; lines 35-58; and Column 14, lines 1-63); and Kyle discloses that the program logic is adapted to perform this at least one security check of a playback device seeking to play the audiovisual content, the at least one security check adapted to verify at least one of playback device identity, including at least one of a player serial number, specific subscriber information, player model, or player software version, or a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 24; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 23,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the device of claim 12, in addition, Asano discloses logic that performs a security check that interrogates a playback environment to verify at least one of playback device identity, including at least one of a player serial number, specific subscriber information, player model, or player software version, or a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device (Column 6, lines 29-32; Column 8, lines 45-59; Column 9; lines 35-58; and Column 14, lines 1-63).

Regarding Claim 24,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the device of claim 12, in addition, Kyle discloses that the Turing-complete interpreter is adapted to execute program logic (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 24; and Column 7, line 59 to Column 8, line 5); and Nonaka discloses program logic that does not decrypt a selected version if the program logic identifies the media as revoked (Paragraphs 232-234).

Regarding Claim 25,

Asano as modified by Benaloh, Nonaka, and Kyle discloses the method of claim 16, in addition, Asano discloses at least one security check adapted to verify at least one of playback device identity, including at least one of a player serial number, specific subscriber information, player model, or player software version, or a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised player and to inhibit at least one of full quality playback or playback if at least one security check fails (Column 6, lines 29-32; Column 8, lines 45-59; Column 9; lines 35-58; and

Column 14, lines 1-63); and Kyle discloses that the program logic performs this at least one security check of a player device seeking to play the audiovisual content, the at least one security check adapted to verify at least one of playback device identity, including at least one of a player serial number, specific subscriber information, player model, or player software version, or a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised player and to inhibit at least one of full quality playback or playback if at least one security check fails (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 24; and Column 7, line 59 to Column 8, line 5).

5. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh, Nonaka, and Kyle, further in view of Sugahra (EP 0 668 695 A2).

Asano as modified by Benaloh, Nonaka, and Kyle does not explicitly disclose means for reducing during a rendering process the output quality of the audiovisual content in dependence upon whether a security requirement by the medium for high quality output is met.

Sugahra, however, discloses means for reducing during a rendering process the output quality of the audiovisual content in dependence upon whether a security requirement by the medium for high quality output is met (Column 9, line 50 to Column 12, line 4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data quality altering system of Sugahra into the information recording/reproducing system of Asano as modified by Benaloh, Nonaka, and Kyle in order to allow the device to alter the content that is displayed based on numerous factors, including country, rating, viewer's age, device's and medium's protection levels, and the like, thereby allowing a single piece of content to be viewed in many different forms dependent upon the above.

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh, Nonaka, and Kyle, further in view of Foote (U.S. Patent 6,164,853).

Asano as modified by Benaloh, Nonaka, and Kyle discloses the method of claim 16, in addition, Kyle discloses that the interpreter performs operations specified in the program logic to respond to selections from a user (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5), but does not explicitly disclose that the user selections include button presses on a remote control.

Foote, however, discloses that the user selections include button presses on a remote control (Column 1, lines 25-39). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the remote of Foote into the information recording/reproducing system of Asano as modified by Benaloh, Nonaka, and Kyle in order to enable a user to operate the player from the comfort of the user's chair or sofa, thereby eliminating the need to physically interact with the player itself.

7. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh, Nonaka, and Kyle, further in view of Ford (Ford, Susan, "Advanced Encryption Standard (AES) Questions and Answers", 10/2/2000, pp. 1-5, obtained from http://www.nist.gov/public_affairs/releases/aesq&a.htm).

Asano as modified by Benaloh, Nonaka, and Kyle discloses the method of claim 16, in addition, Kyle discloses that the program logic directs the player to perform a cipher operation via an interpreter (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5); but does not disclose that the cipher operation is an AES cipher operation.

Ford, however, discloses that the cipher operation is an AES block cipher operation (Pages 1-5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption algorithm of Ford into the information recording/reproducing system of Asano as modified by Benaloh, Nonaka, and Kyle in order to use an encryption algorithm that provides high security, performance, efficiency, ease of implementation, and flexibility and that is easy to defend against power and timing attacks.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437